A Cybersecurity Handbook for NFPs

March 2025

Contents

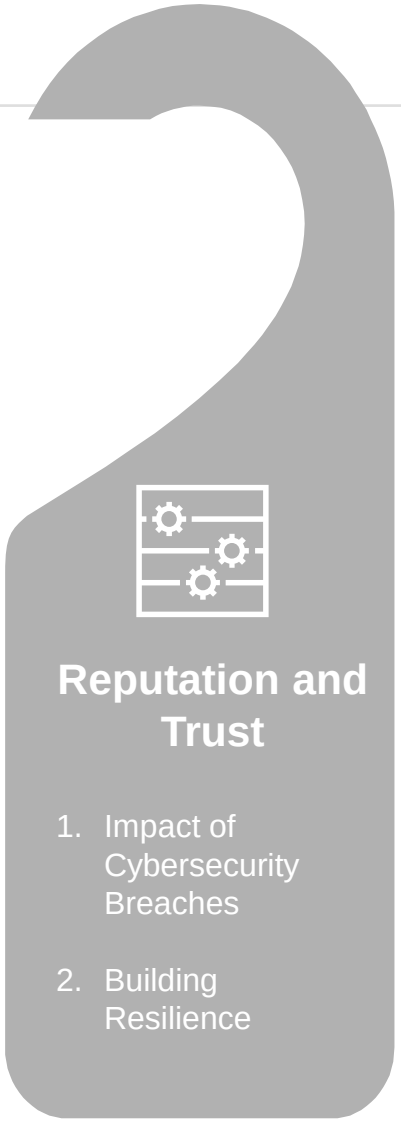
Importance of Cyber for NFP's

Growing Digital Reliance

1. Digital Platforms in Operations
2. Fundraising and Service Delivery

Sensitive Data Handling

1. Responsibility for Data Protection
2. Data Security Measures



Reputation and Trust

1. Impact of Cybersecurity Breaches
2. Building Resilience

Regulatory Compliance

1. Adherence to Data Protection Regulations
2. Maintaining Stakeholder Trust

Understanding Risks and Vulnerabilities

We frequently conduct the following approach with our clients to identify and assess information security and cyber risks, to enable enhanced visibility and clarity into the cyber risk profile and outline the relationships between threats, risks, controls and vulnerabilities.

Identify Threats → **Identify Risks** → **Identify Controls** → **Identify Vulnerabilities (Issues and Gaps)** → **Identify Remediation and Uplift Activities**

Threat Scenarios

Understanding the **adversaries,** their **motives** and their **targets** allows us to understand common threat scenarios that could affect an organisation.

We typically build these into **threat scenarios**.

Cyber Risks

Cyber Risks are the potential for digital threats to occur that could compromise your organisation's information security and privacy.

Inherent Risk is used to **measure** the risk to an organisation in the absence of any controls.

Cyber Controls

Controls help mitigate the threats and risks and help an organisation to understand their **residual risk.**

Cyber controls are normally a mixture of technical and non-technical controls. *e.g. Training and Awareness & Multi-factor authentication.*

Gaps & Vulnerabilities

Controls are assessed or tested to identify weaknesses, failures or areas for improvement in our controls.

Technical vulnerabilities may also be informed by any existing Threat Intelligence and the technology environment.

Remediation Actions

For each gap identified, actions should be **documented** and **assigned owners** for remediation.

Actions should be **prioritised** for completion, based on factors like cost, dependencies and contribution to mitigating the risk.

Types of Threat Actors

What we see most commonly in the NFP sector (e.g. phishing and ransomware attacks)

Espionage (Nation States)

Espionage threat actors (often referred to as "Advanced Persistent Threats", or APTs) typically seek to steal information which will provide an economic or political advantage to their benefactor

Criminal/Financially Motivated

Cyber criminal groups usually have one goal: profit. Whether it be through sophisticated ransomware operations or a data breach incident, these groups are a danger to all organisation's

Hacktivist

Hacktivists conduct attacks to increase their public profile and raise awareness of their cause. They attempt to achieve this aim through a multitude of methods, ranging in sophistication

Sabotage

Saboteurs seek to damage, destroy, or otherwise subvert the integrity of data and systems. Sabotage attacks are not always deliberate and have been used to mask other malicious activity

The Threat Landscape

Adversaries

- Nation State
- Terrorists
- **Cybercriminals**
- Hacktivists
- Insiders

Motives

- **Financial gain**
- Influence social or business change
- Patriotism
- Economic and/or military advantage
- Personal or professional revenge

Targets

- Corporate/ trade secrets
- Ideological supporters
- Critical infrastructure
- Emerging technologies
- **Confidential information**

Key Risks

Confidentiality	**Data leakage or theft** Externalisation of confidential data/information
Integrity	**Data manipulation** Unauthorised modification of data/information
Availability	**Service Disruption** Unavailability of data/information of processes to perform operations
Privacy and Data	**Misuse of personal data** Mismanagement of data or violation of regulatory privacy obligations

Measuring Cybersecurity Risk

Identify Threats → Identify Risks → Identify Controls → Identify Vulnerabilities (Issues and Gaps) → Identify Remediation and Uplift Activities

Once an organisation has identified their cybersecurity risks, it is critical to understand how to assess those risks and bring down the risk profile.

Identify the threat scenarios
*e.g. We are worried about getting phished and losing **confidential data***

→ **Inherent Risk**

Identify existing controls.

e.g. Do we have training in place? Do we have a cyber policy?

→ **Current (Residual) Risk Rating**

Identify and address known gaps and vulnerabilities.

e.g. Are people doing their cyber training?

→ **Target (Residual) Risk Rating**

Identify long-term initiatives for uplift.

e.g. Can we automatically enforce our cyber training annually?

→ **Risk Appetite Level**

Current State

Increase in Cyber Spend & Investment

Target State

Assessing Risk – Risk Profile

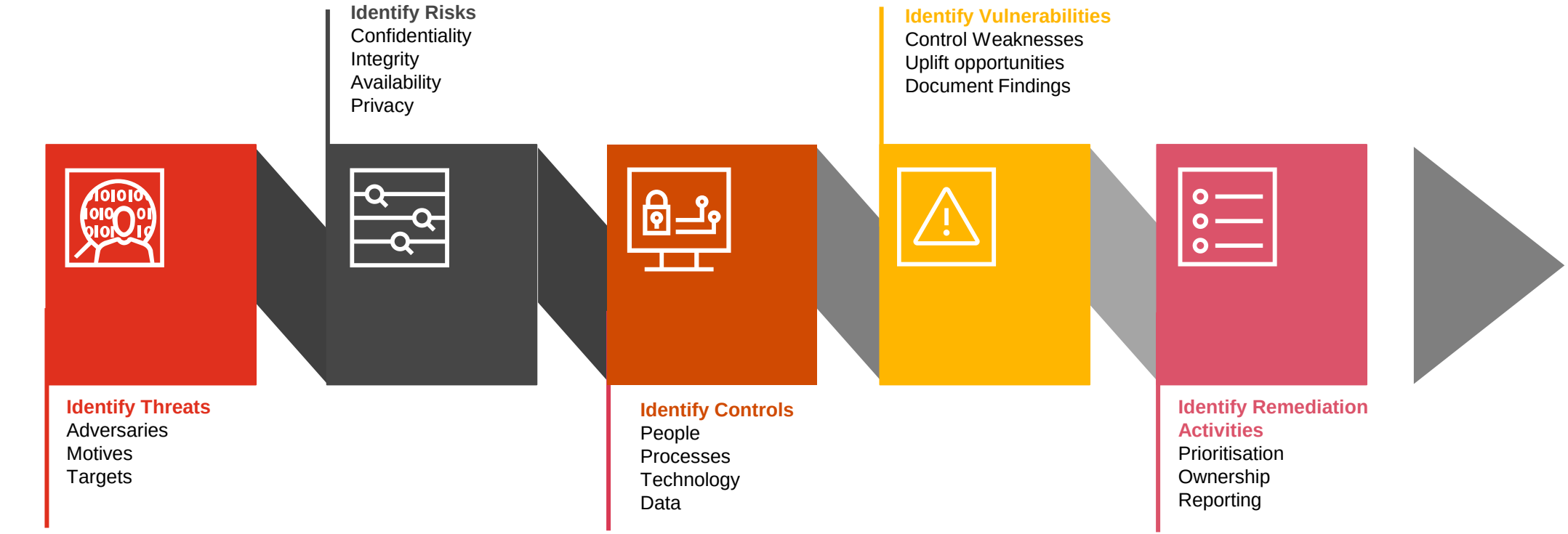
Consequence					
Extreme	Medium	High	High	Critical (A)	Critical (C)
Major	Medium	Medium	High (A)	Critical (I)	Critical (C)
Medium	Low	Medium	Medium (A)	High	High
Minor	Very Low	Low	Low (I)	Medium (C)	High
Insignificant	Very Low	Very Low	Low	Low	Medium
	Rare	Unlikely	Possible	Likely	Almost Certain

Likelihood

Legend

- C — Confidentiality
- I — Integrity
- A — Availability
- Current Inherent Risk Rating
- Current Residual Risk Rating
- Target Residual Risk Rating
- Risk Appetite Level

Understanding Risks and Vulnerabilities (takeaway)



- Assessing your risks comes down to understanding what controls you have in place.
- Documenting issues and actions is the key to success! Risk won't get reduced without oversight and ongoing reporting of progress.
- It's impossible to solve everything all at once – prioritise and work on what can be done.

Common Shortfalls

Let's look at a scenario. Consider a large financial organisation who wants to stay on top of all the new technologies and with their increased cyber budget have opted to purchase the Microsoft Cybersecurity Suite.

Positives

- **Innovation and Growth**
- **Increased Efficiency**
- **Enhanced Capabilities**
- **Scalability**

Negatives

- **Duplicate Capabilities**
  - New tools may offer features already available in existing solutions, leading to redundancy.
- **Increased Costs**
  - Initial purchase, training, and maintenance of new technologies can strain budgets.
- **Underutilization**
  - Organizations often invest in tools without fully leveraging their capabilities, wasting resources.

Cost Effective Cyber Risk Mitigation

What can you start doing now, to help reduce your cyber risk?

Prioritise enhancements that directly support organisational objectives.

Invest in understanding and utilising existing tools to their fullest potential before seeking new solutions.

Adopt a balanced approach that combines necessary new investments with optimisation of current resources.

Educate your employees

Social engineering attacks are the most prevalent cybersecurity threat

Cyber Governance

Create clear roles and responsibilities. Reference and leverage procedures available online

Incident Response Plans

Ensure you are prepared for a cyber incident

Vendor and Third-Party Risk Management

Ensure you are working with organisations who also prioritise cybersecurity

ACSC Essential Eight

Application Control

Patch Applications

Configure Microsoft Office Macros

User Application Hardening

Restrict Administrative Privileges

Patch Operating System

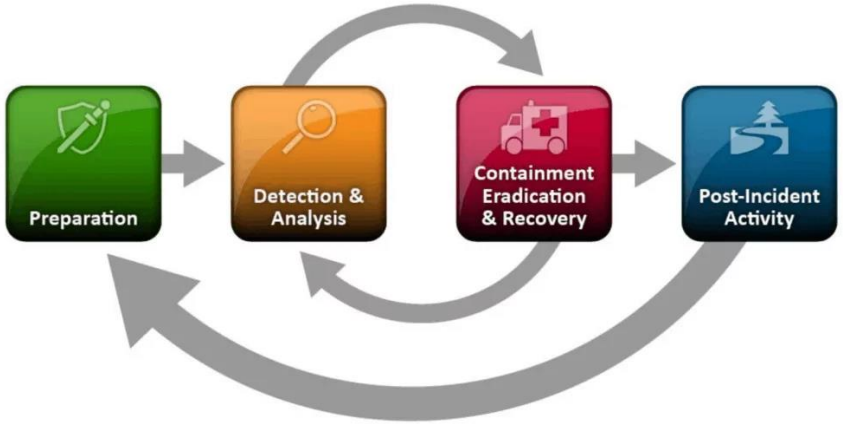
Multi Factor Authentication

Regular Backups

Incident Response Plan

Take these identified threats, risks and vulnerabilities and develop an incident response plans based on these. At a minimum your incident response plan should follow:

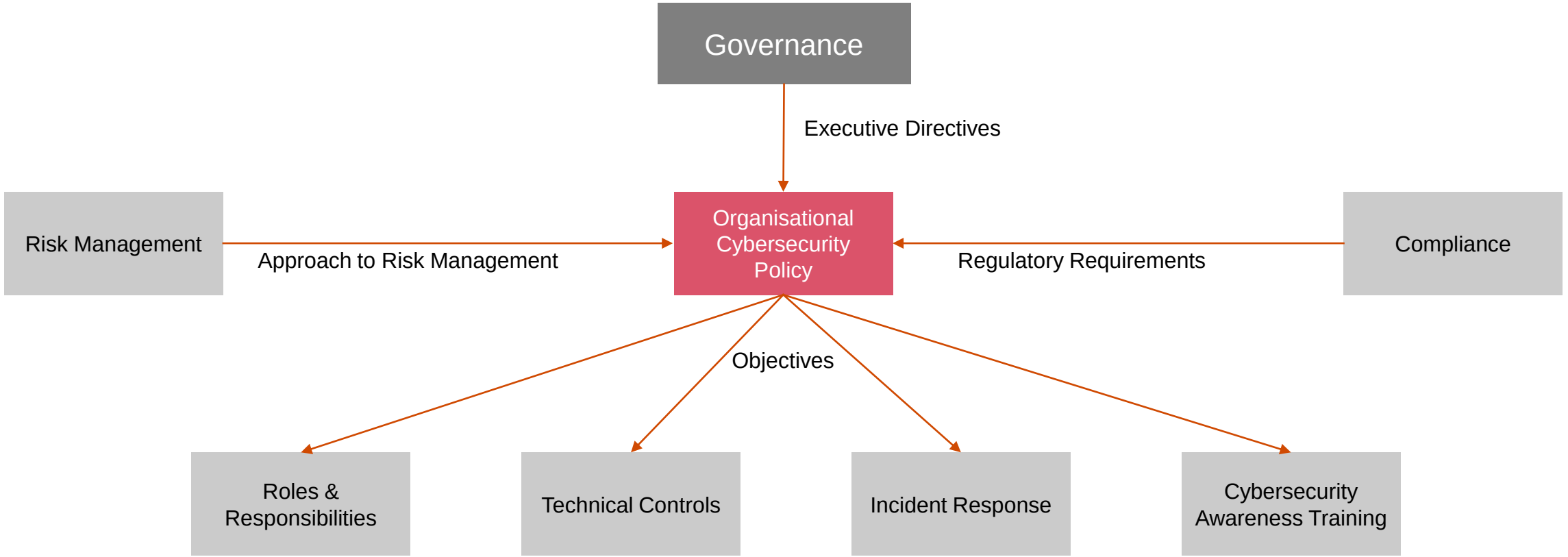
1. **Preparation**
   - Assigned roles to team members
   - Communication guidelines
2. **Detection & Analysis**
   - Incident Classification (i.e. so you know how to prioritise)
3. **Containment, Eradication & Recovery**
   - Immediate steps to limit damage (e.g. system isolation)
   - Procedures for removing threats and unauthorised access
   - Clear steps for data backup and system restoration
4. **Post-Incident Activity**
   - Lessons learnt activity



Note: If you have threats you are particularly worried about then specific "playbooks" can be created to help streamline your response in this scenarios. Playbooks enable more precise and clear steps that can be followed in extreme scenarios, e.g. ransomware incidents.

Policy

What should our policy include and what is it trying to achieve?



Implementation Guidance (direct from the Policy)

[Insert Company Logo Here]

Information Security Policy

Version - 0.1

Effective Date: << Date Month Year>>

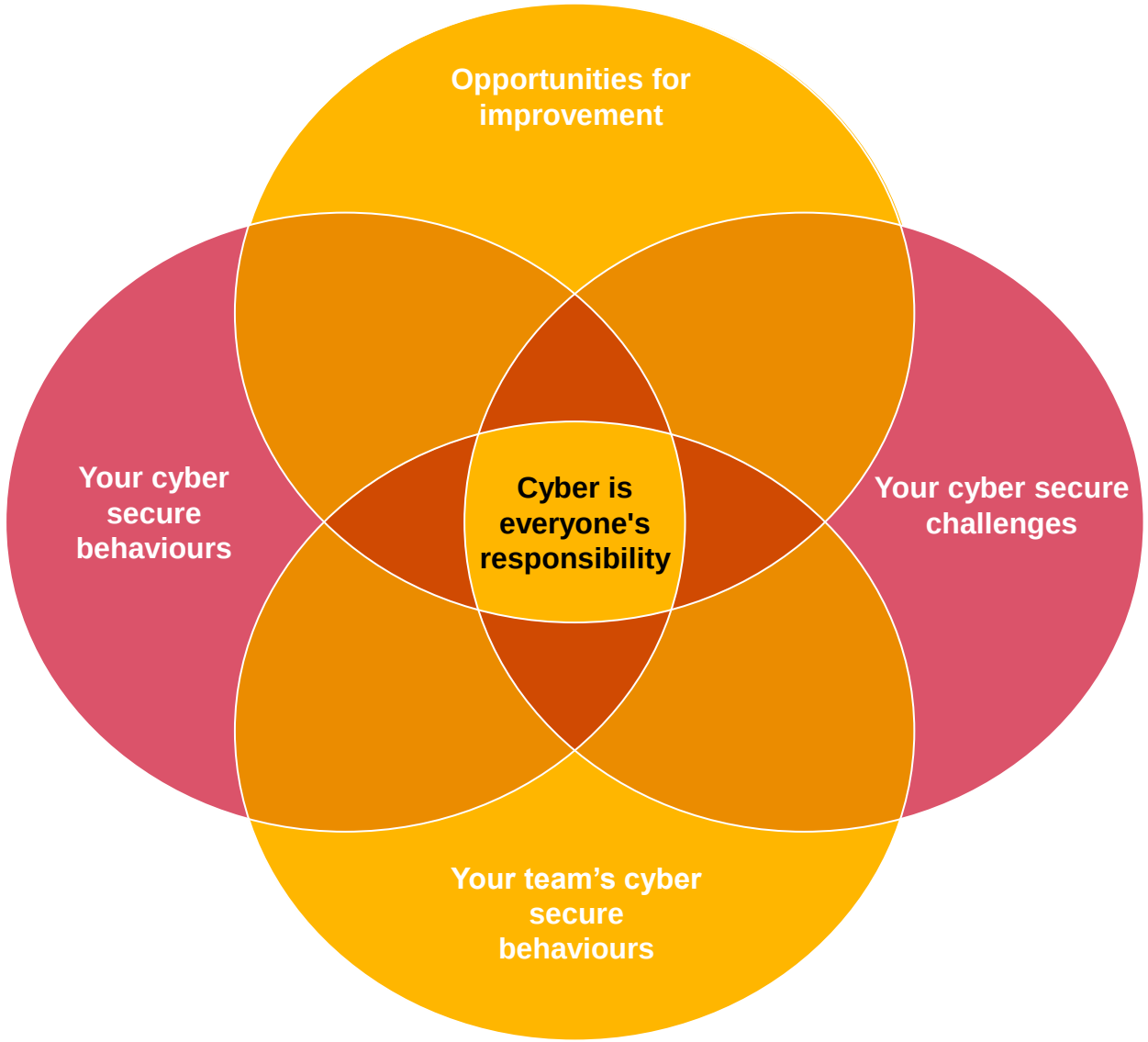
Table of Contents

Key Strategy Controls:

1. Application Control
2. Patch Applications
3. Patch Operating Systems
4. Configuration Microsoft Office Macros
5. Microsoft Office Macro Hardening
6. Multi-factor Authentication
7. Backup/Recovery
8. Awareness and Training
9. Incident Response
10. Physical Security
11. Risk Assessment
12. NIST Risk Management Framework
13. Password Management

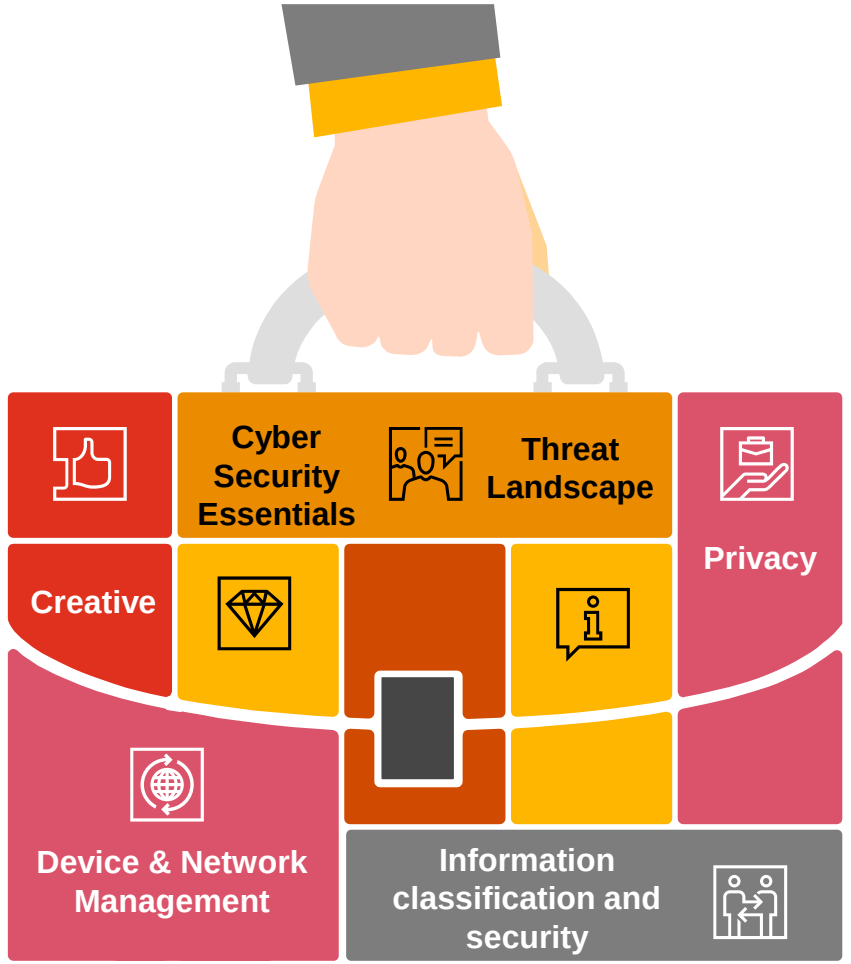
(further elaboration in the Policy)

Training staff and volunteers



Designing Cyber Awareness Training Programs

Goal:
Create and leverage a program that is engaging and relevant



Free Resources

General Cyber Resources

Digital Transformation Hub

Infoxchange Digital Transformation Hub

Contains many links to guides, advice, and information that can help improve cyber security practices in your organisations. Resources are broken down into three levels; Basic, Intermediate, and Advanced.

View the Report here: https://www.infoxchange.org/au/digital-technology-not-for-profit-sector

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

ACSC Small Business Cyber Security Guide

This guide has been developed to help small businesses protect themselves from the most common cyber security incidents.

ASD Cyber Checklist for charities and not-for-profits

This checklist has been developed to help charities and non-profits improve cyber security through easy-to-follow steps and links to best practice advice.

ACSC Step-by-step Guides

The Guide to undertaking privacy impact assessments (PIA Guide) has been prepared by the Office of the Australian Information Commissioner (OAIC) to describe a process for undertaking a privacy impact assessment (PIA).

Australian Government | Australian Charities and Not-for-profits Commission

ACNC Governance Toolkit: Cybersecurity

Governance Toolkit - helps to understand cybersecurity issues - what they are, how they may affect charities and what charities can do to reduce risks of cyber attacks.

Free Resources for NFPs

Understanding privacy obligations

Understanding the Notifiable Data Breaches Scheme

Fact sheet that contains information on the Notifiable Data Breaches Scheme, including how to notify and penalties for not complying.

Privacy Compliance Manual

Norton Rose Fulbright has provided Not-for-profit Law, a service of Justice Connect, with its Privacy Compliance Manual for use by charities and not-for-profits. The Manual contains an overview of new federal privacy laws and a template privacy policy.

Guide to undertaking privacy impact assessments

The Guide to undertaking privacy impact assessments (PIA Guide) has been prepared by the Office of the Australian Information Commissioner (OAIC) to describe a process for undertaking a privacy impact assessment (PIA).

Privacy Guide - A guide to complying with privacy laws in Australia

This guide is for not-for-profit organisations in Australia who want to understand more about their obligations under privacy laws in Australia. This guide describes obligations under the Privacy Laws.

Responding to incidents

Cyber Incident Response Guide

This document provides guidance, resources, and security practices to help organisations prepare and respond to cyber incidents.

Report Cyber Incidents

Use this website to report any cyber incidents to the ACSC.

Sample Incident Response Template

A Cyber Incident Response Plan template developed by the Victorian Government that can be leveraged to create a plan for any organisation.

OAIC Notifiable Data Breach

The website of the Office of the Australian Information Commissioner where Notifiable Data Breaches must be reported.